This work was supported in part by the Spanish Ministry of Economy and Competitiveness under TestEAMoS (TIN2016-76956-C3-1-R) project and ERDF funds.

Test Driven Anonymization Technique for Artificial Intelligence

Cristian Augusto, Jesús Morán, Claudio de la Riva and Javier Tuya
Software Engineering Research Group
http://giis.uniovi.es
University of Oviedo

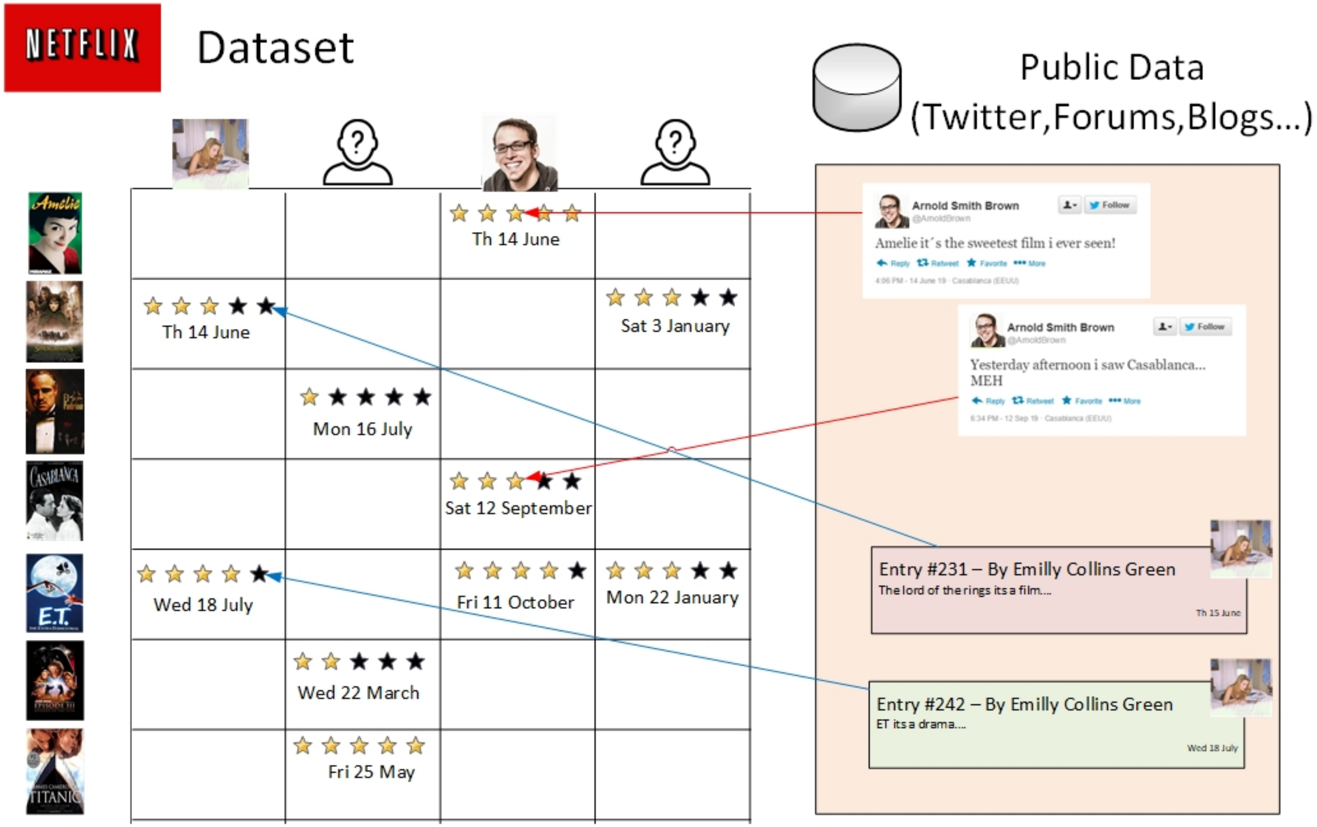
Netflix Contest Dataset (I)

NETFLIX Dataset

	?	?	?	?
			⭐⭐⭐⭐⭐ Th 14 June	
	⭐⭐⭐★★ Th 14 June			⭐⭐⭐★★ Sat 3 January
		⭐★★★★ Mon 16 July		
			⭐⭐⭐★★ Sat 12 September	
	⭐⭐⭐⭐★ Wed 18 July		⭐⭐⭐⭐★ Fri 11 October	⭐⭐⭐★★ Mon 22 January
		⭐⭐★★★ Wed 22 March		
		⭐⭐⭐⭐⭐ Fri 25 May		

- Release an useful dataset without identifiers to develop recommenders with it

Netflix Contest Dataset (II)



		☆☆☆☆☆ Th 14 June	
☆☆☆★★ Th 14 June			☆☆☆★★ Sat 3 January
	☆★★★★ Mon 16 July		
		☆☆☆★★ Sat 12 September	
☆☆☆☆★ Wed 18 July		☆☆☆☆★ Fri 11 October	☆☆☆★★ Mon 22 January
	☆☆★★★ Wed 22 March		
	☆☆☆☆☆ Fri 25 May		

Arnold Smith Brown
@ArnoldBrown

Amelie it´s the sweetest film i ever seen!

4:06 PM - 14 June 19 · Casablanca (EEUU)

Arnold Smith Brown
@ArnoldBrown

Yesterday afternoon i saw Casablanca...
MEH

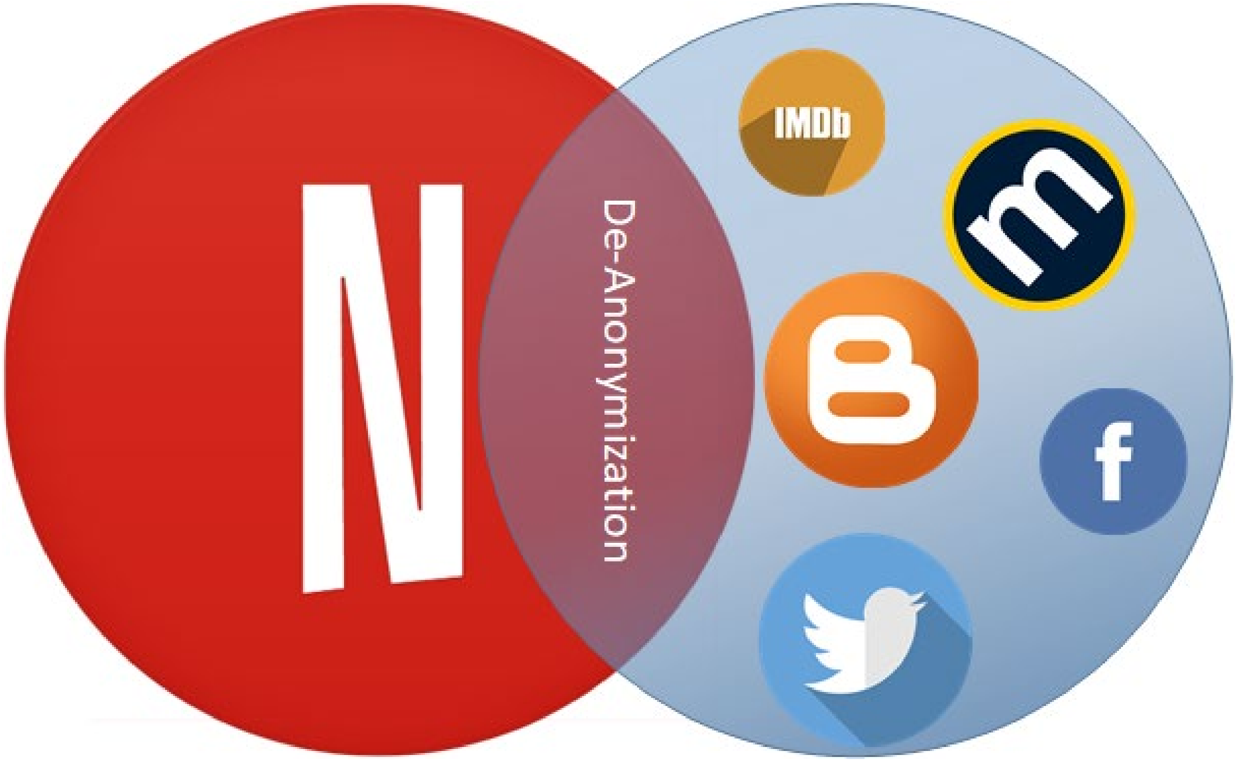
6:34 PM - 12 Sep 19 · Casablanca (EEUU)

Entry #231 – By Emilly Collins Green
The lord of the rings its a film....
Th 15 June

Entry #242 – By Emilly Collins Green
ET its a drama....
Wed 18 July

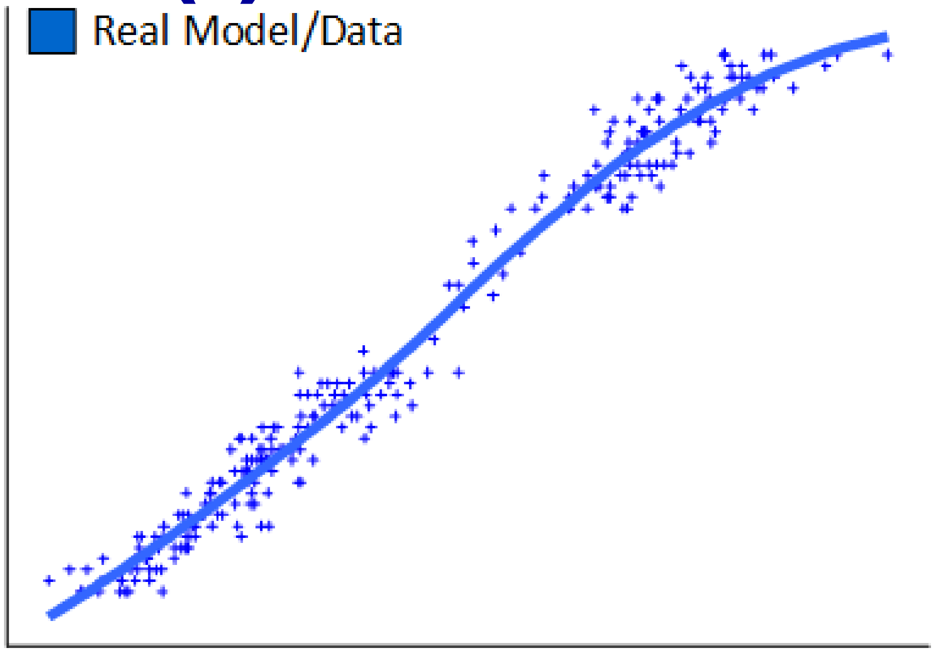
- The information shared by Netflix with another external data like Tweets or Blogs Post allow to identify users

Netflix Contest Dataset (III)



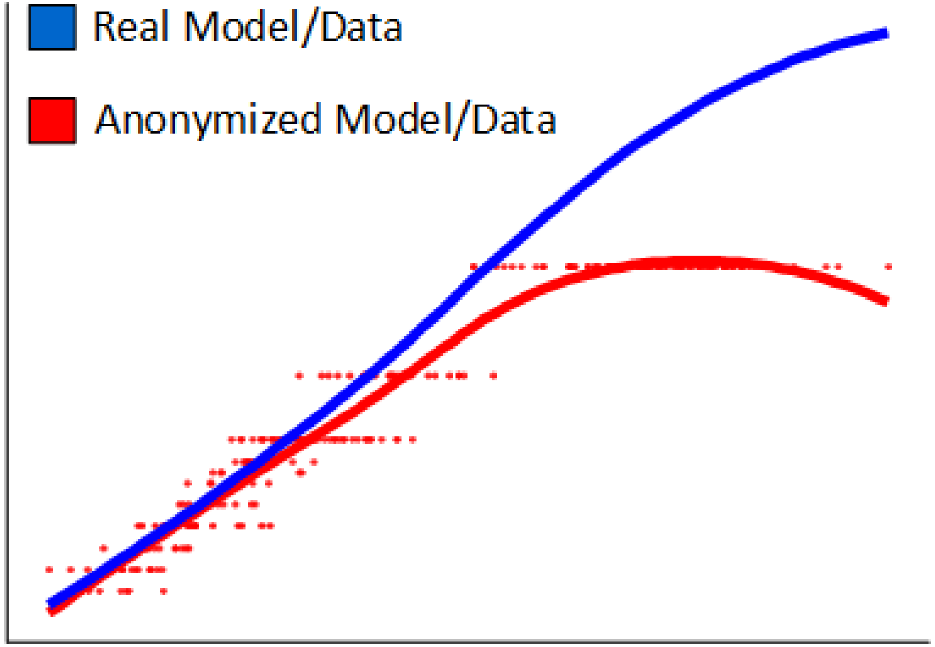
- Cross information of some public sources

Context (I)



- Anonymization effect
  - Improve individuals privacy also loss of information
  - Alters data and affects developments highly dependent of the data (i.e Artificial Intelligence models)

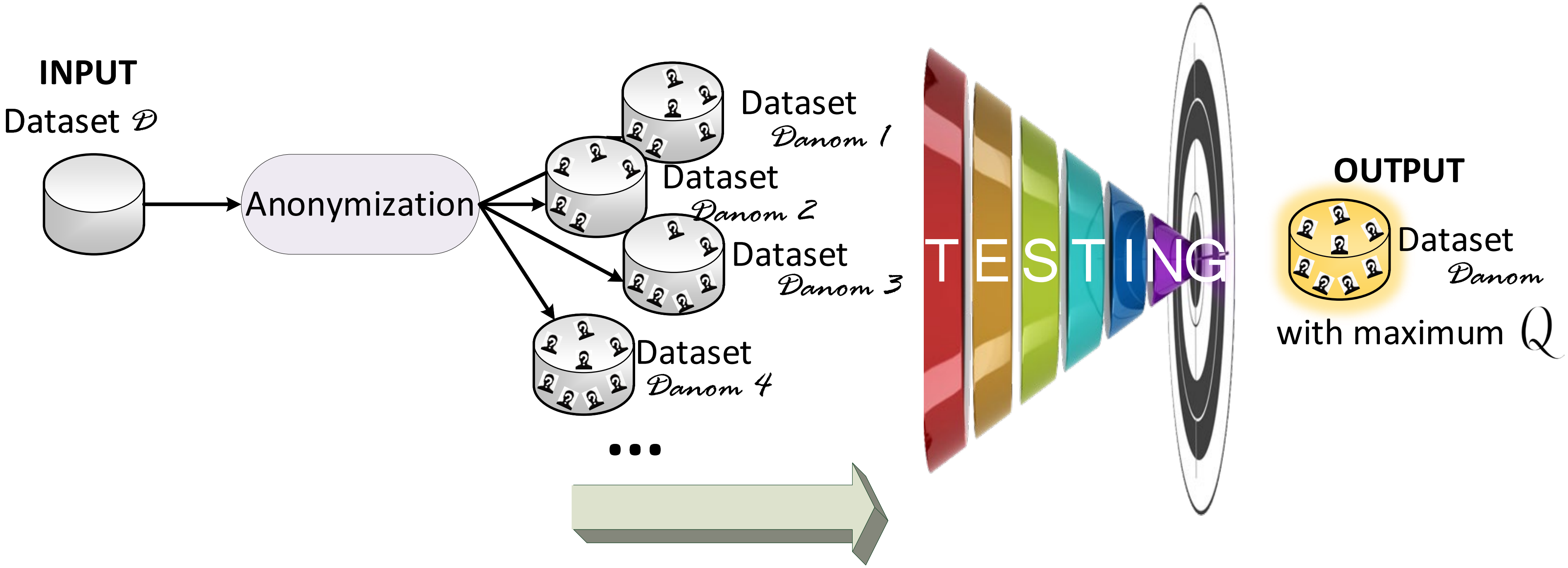
Context (II)



- Fault Masking
  - May be the case that an AI Model that works well in the development stage fails dramatically during production

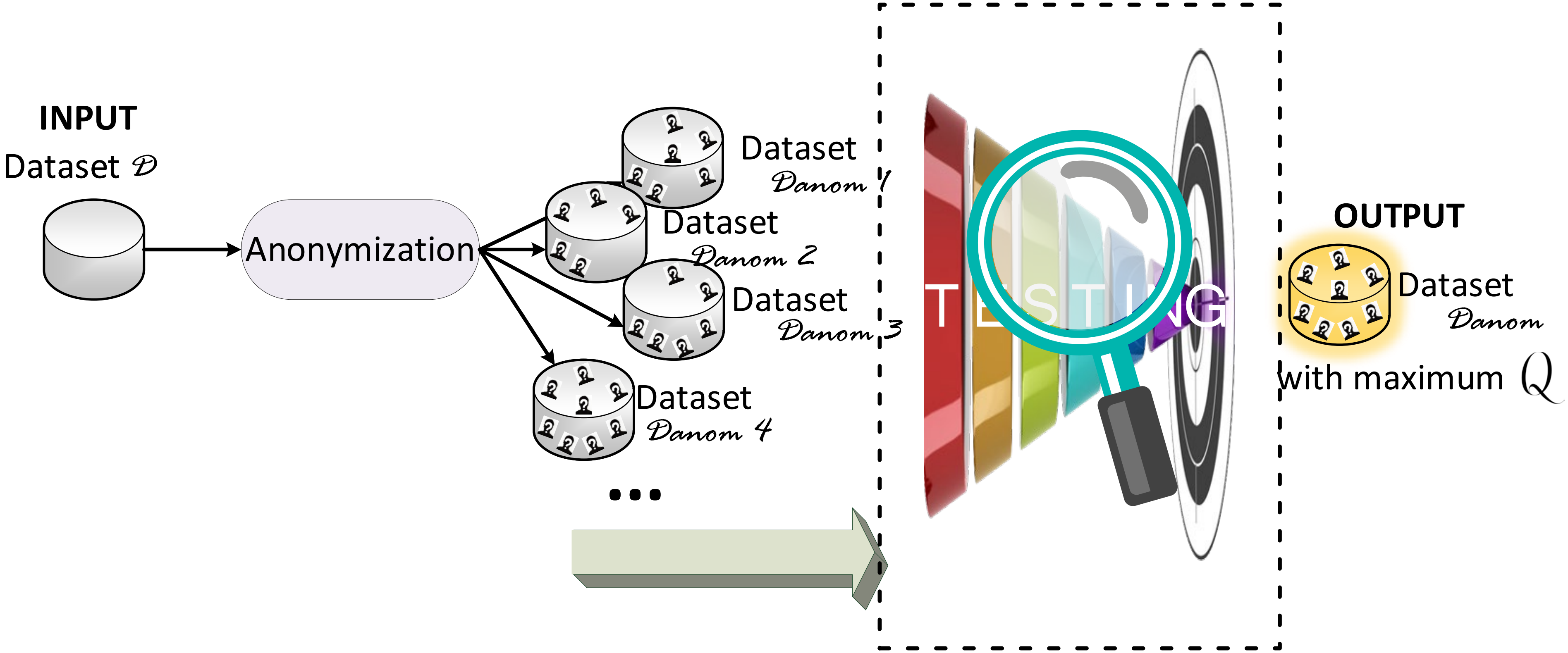
Test Driven Anonymization

Overview



Test Driven Anonymization

Overview



INPUT

Dataset $\mathcal{D}$

Anonymization

Dataset $\mathcal{D}_{anom\ 1}$

Dataset $\mathcal{D}_{anom\ 2}$

Dataset $\mathcal{D}_{anom\ 3}$

Dataset $\mathcal{D}_{anom\ 4}$

…

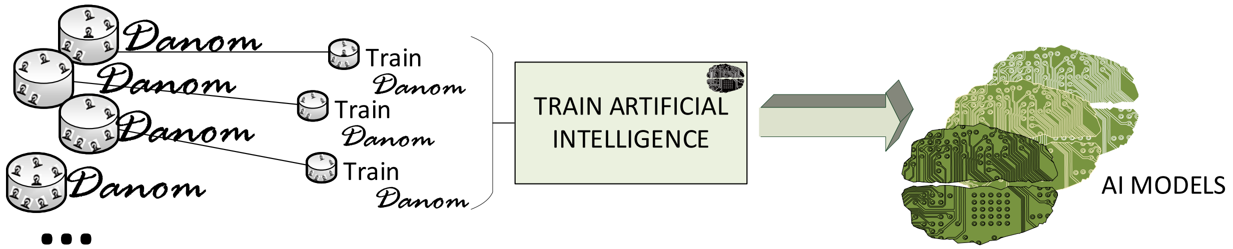
OUTPUT

Dataset $\mathcal{D}_{anom}$

with maximum Q

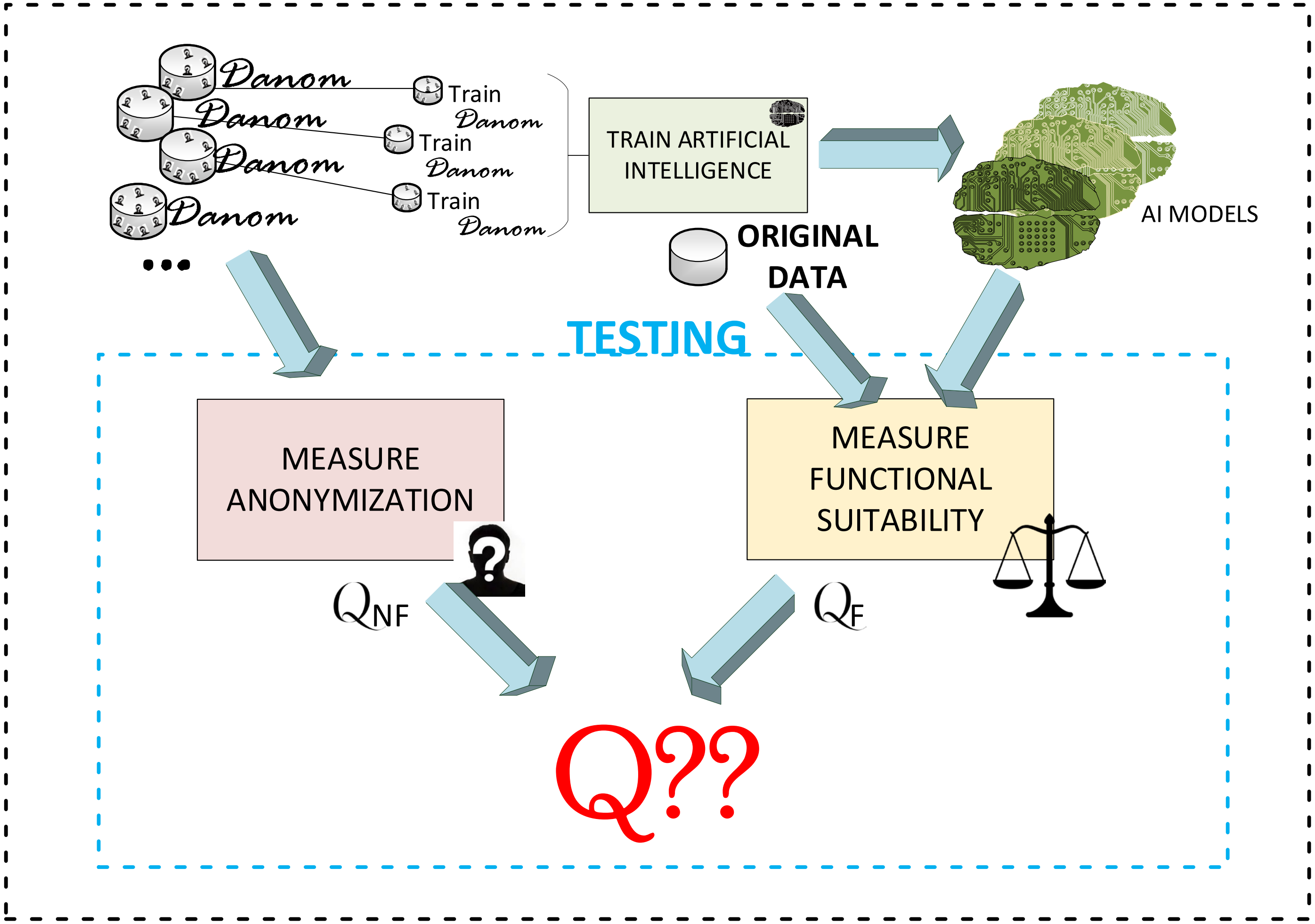
Test Driven Anonymization

Approach



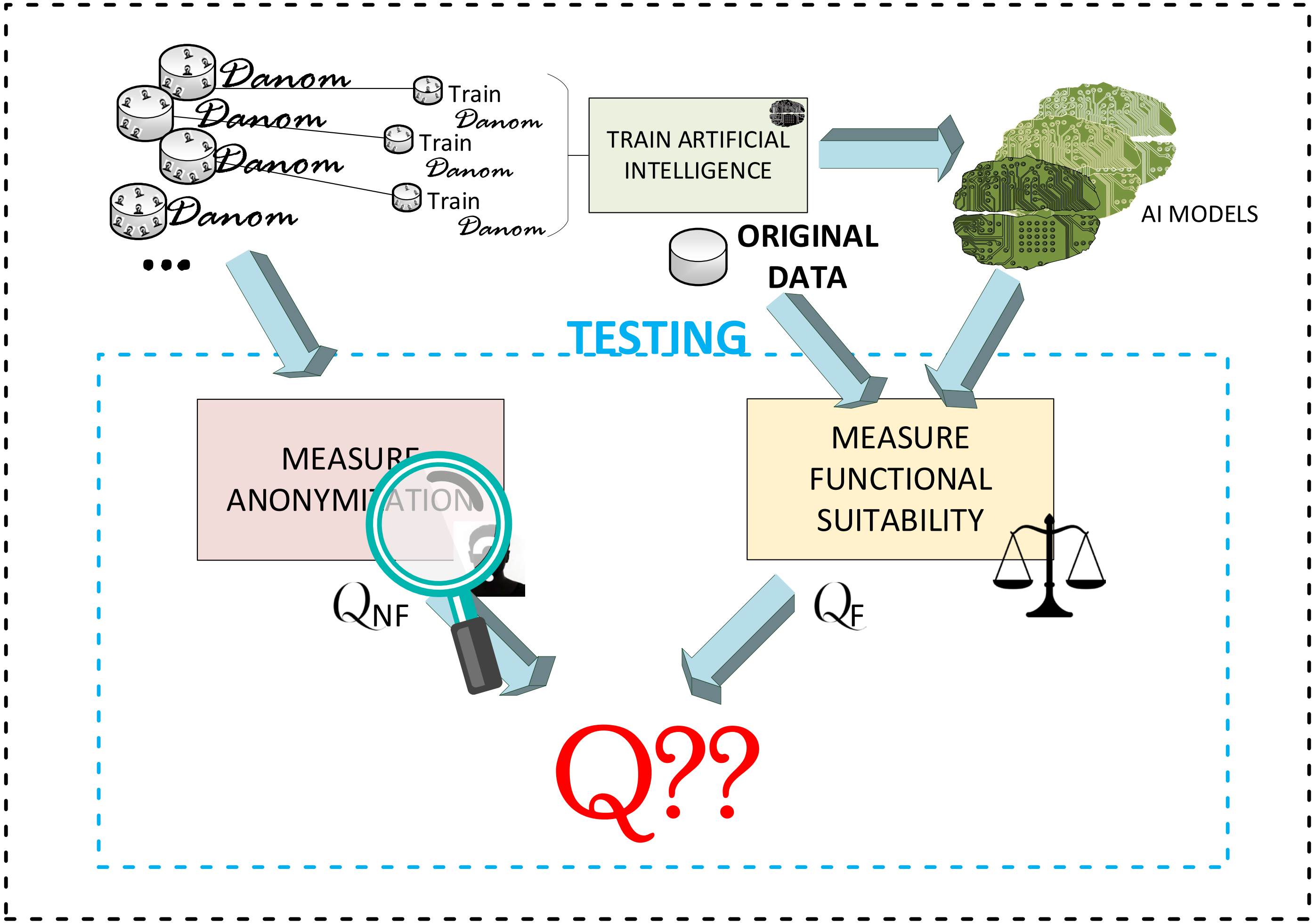
Test Driven Anonymization

Approach



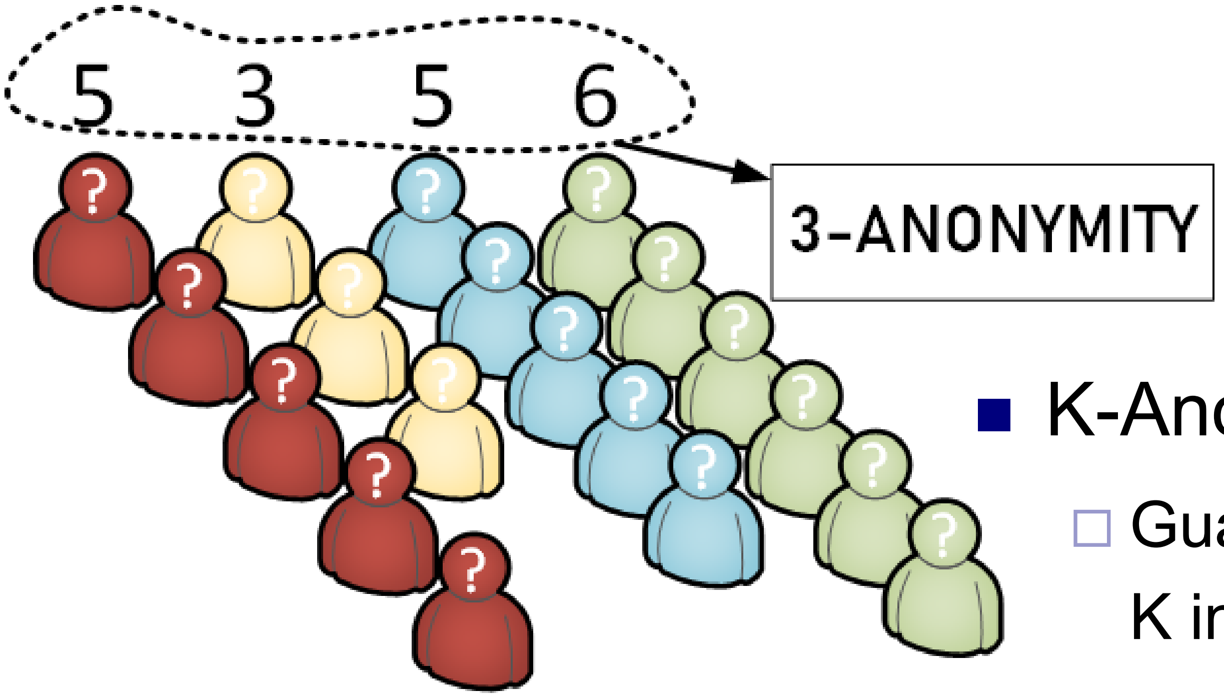
Test Driven Anonymization

Approach



Test Driven Anonymization

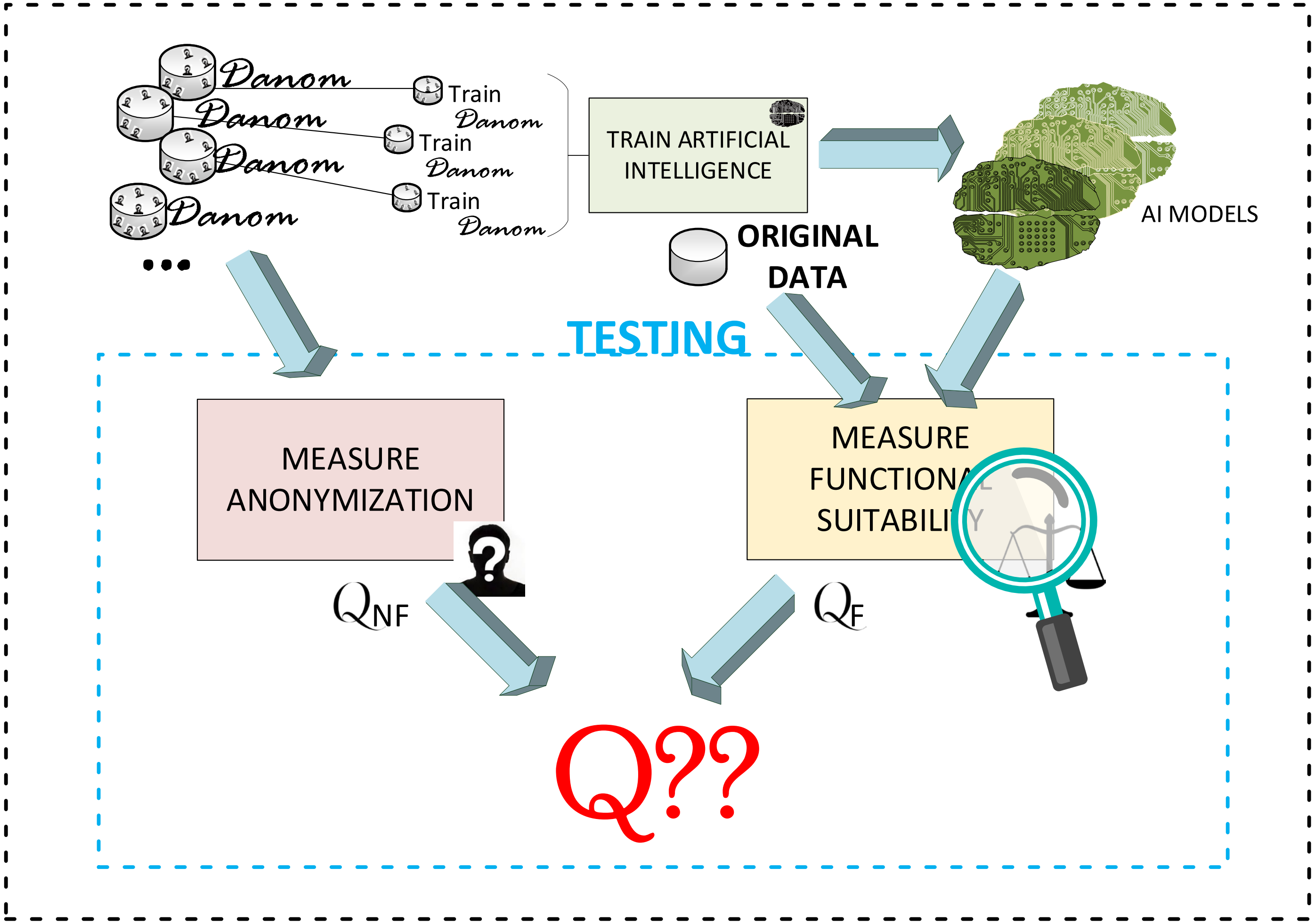
Non-Functional Quality



- K-Anonymity:
  - Guarantees more than K individuals for each combination of pseudo-identifiers

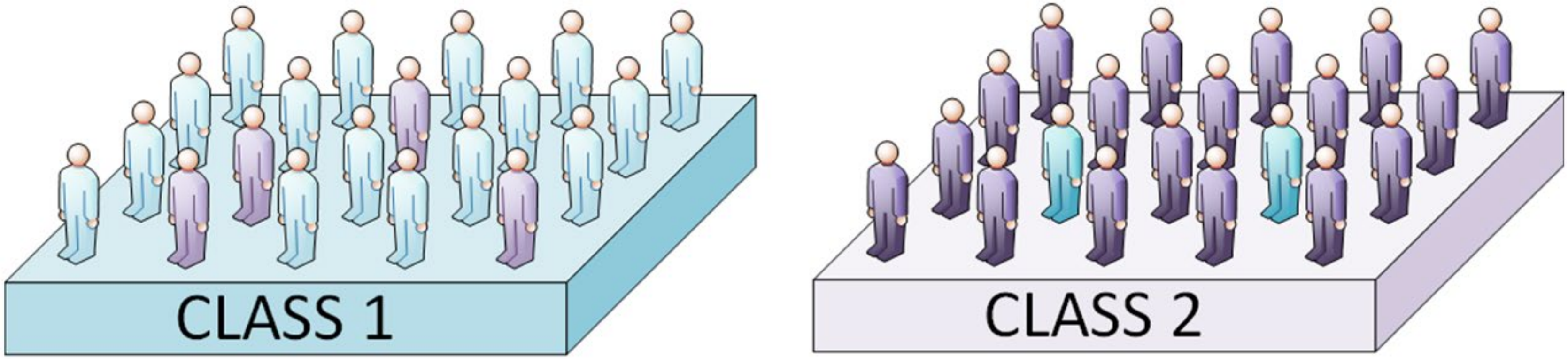
Test Driven Anonymization

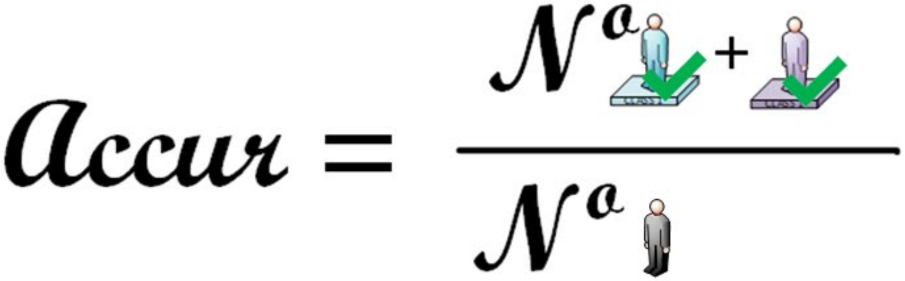
Approach



Test Driven Anonymization

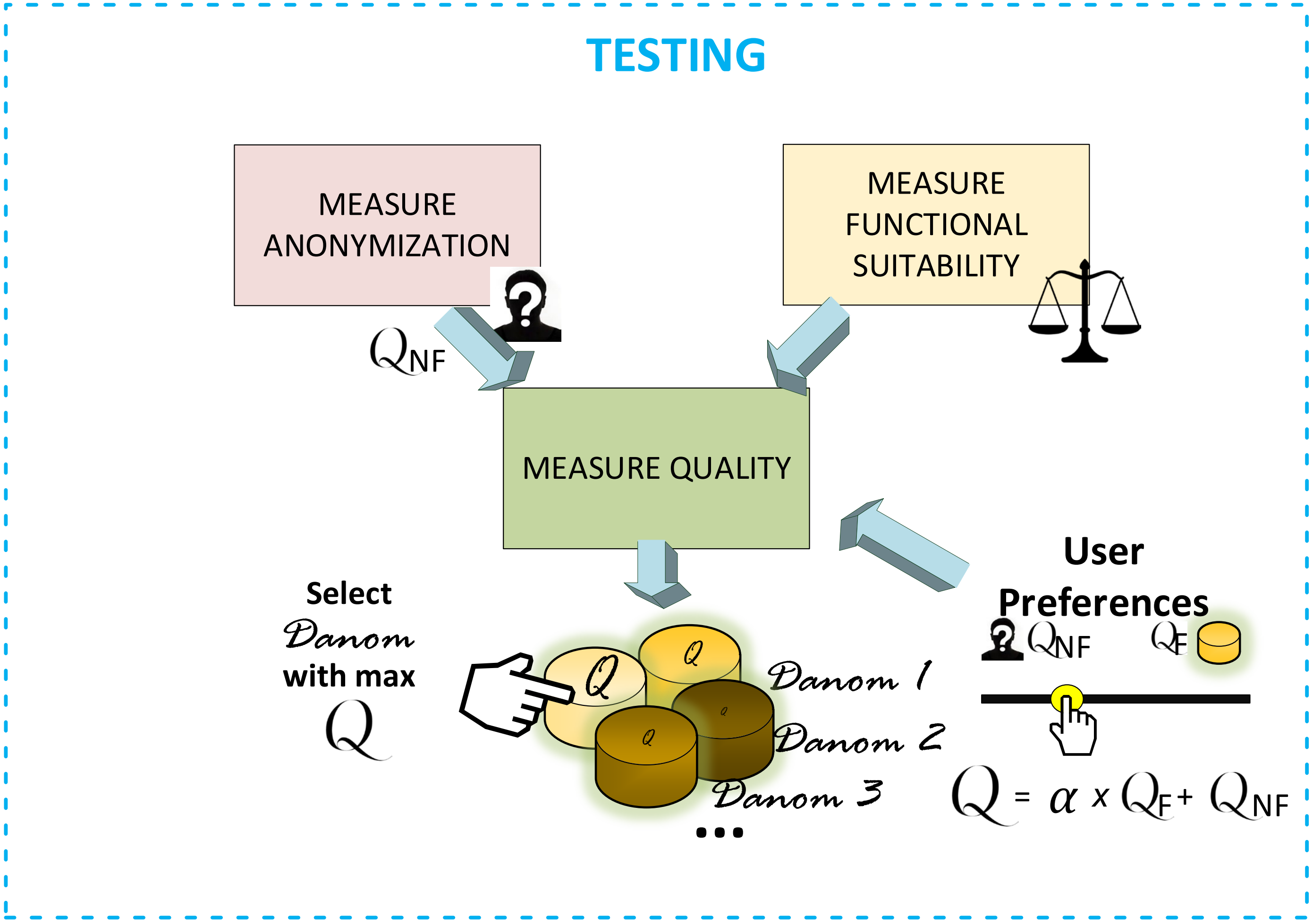
Functional Suitability





Test Driven Anonymization

Quality Metric



TESTING

MEASURE ANONYMIZATION

MEASURE FUNCTIONAL SUITABILITY

Q_{NF}

MEASURE QUALITY

User Preferences

Q_{NF} Q_F

$Q = \alpha \times Q_F + Q_{NF}$

Select Danom with max Q

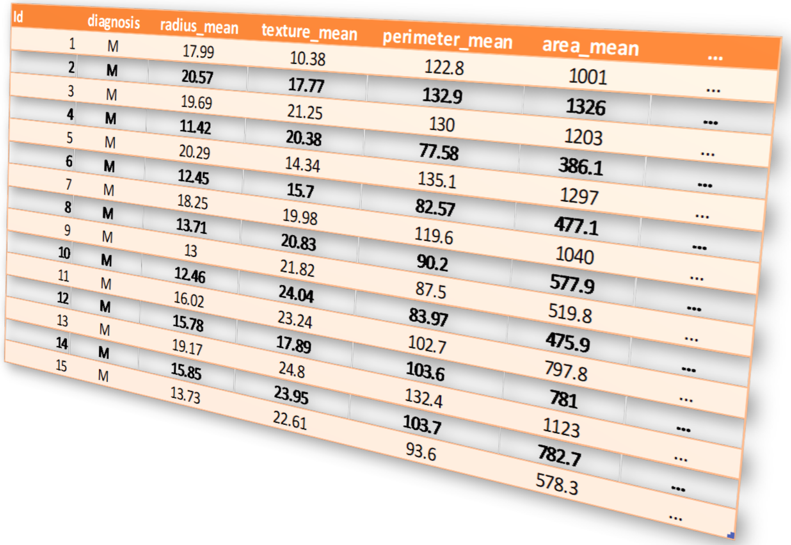
Danom 1

Danom 2

Danom 3

…

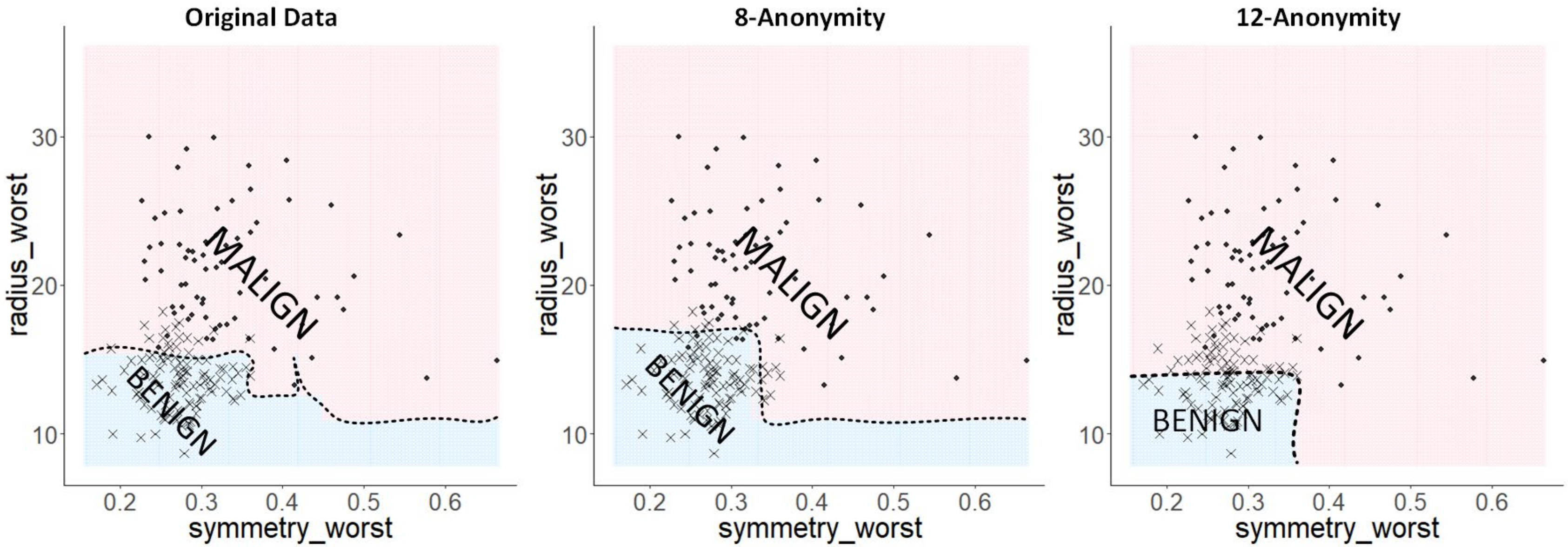
Experimentation (I)



Id	diagnosis	radius_mean	texture_mean	perimeter_mean	area_mean	...
1	M	17.99	10.38	122.8	1001	...
2	M	20.57	17.77	132.9	1326	...
3	M	19.69	21.25	130	1203	...
4	M	11.42	20.38	77.58	386.1	...
5	M	20.29	14.34	135.1	1297	...
6	M	12.45	15.7	82.57	477.1	...
7	M	18.25	19.98	119.6	1040	...
8	M	13.71	20.83	90.2	577.9	...
9	M	13	21.82	87.5	519.8	...
10	M	12.46	24.04	83.97	475.9	...
11	M	16.02	23.24	102.7	797.8	...
12	M	15.78	17.89	103.6	781	...
13	M	19.17	24.8	132.4	1123	...
14	M	15.85	23.95	103.7	782.7	...
15	M	13.73	22.61	93.6	578.3	...

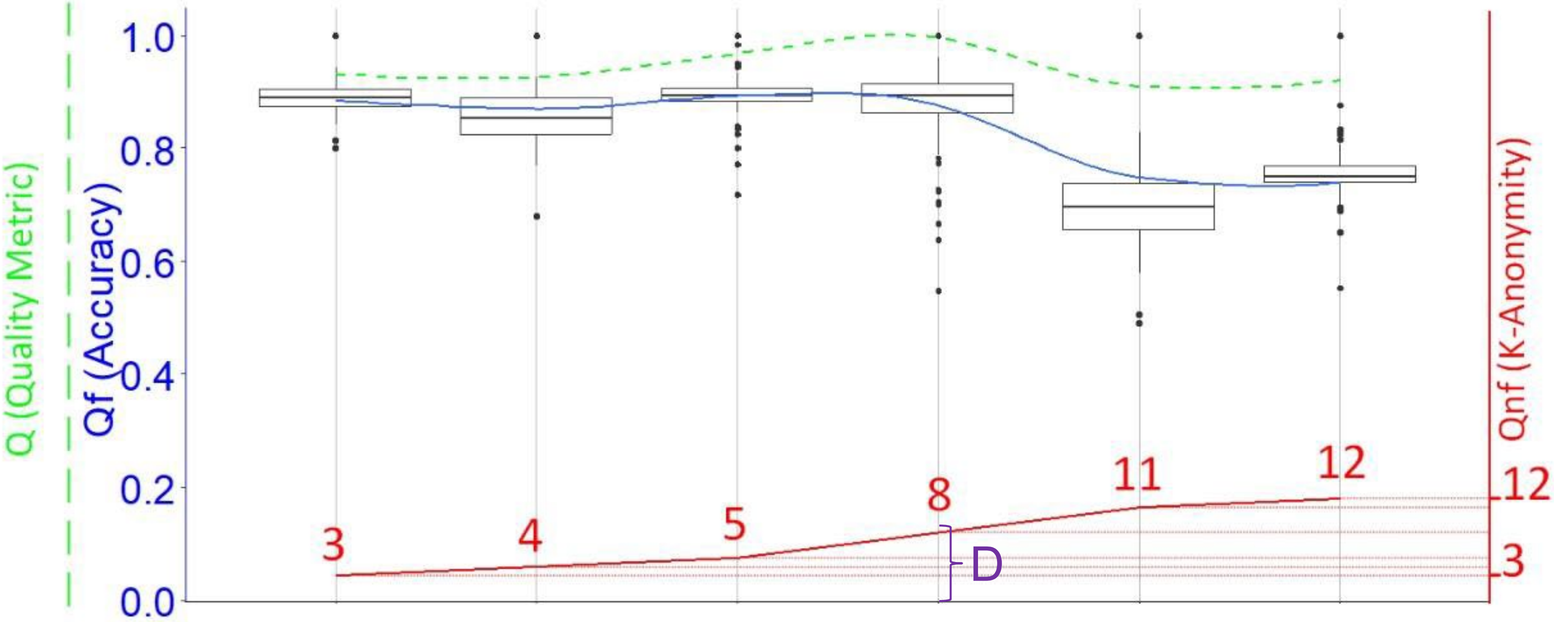
- Two public domain datasets related with medical insurance and health:
  - □ Breast-Cancer(Wisconsin) Dataset
  - □ Medical Cost Personal Dataset
- Using a generalization method with numerical pseudo-identifiers

Experimentation (II)



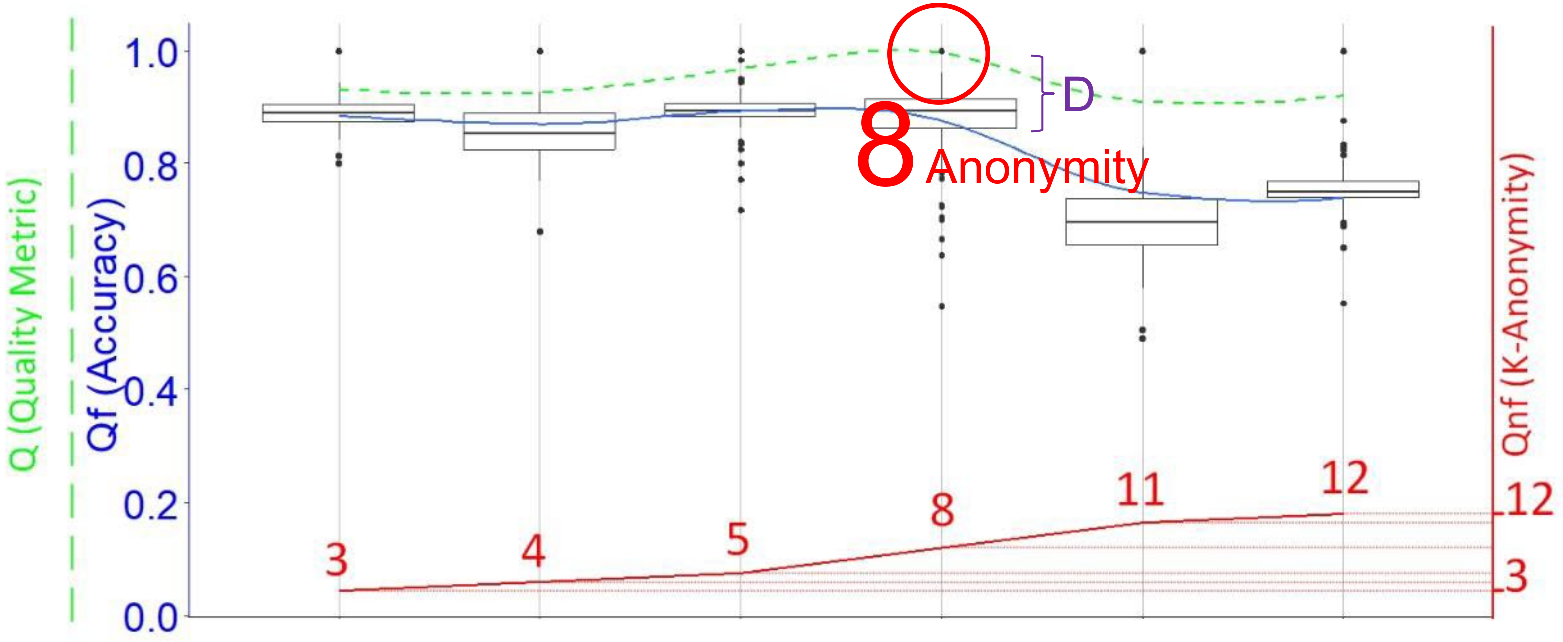
- Wisconsin Dataset:
  - Uses a Random-Forest AI Algorithm for classification, with two size tumor metrics of input
  - Try to predict if the tumor is malign or benign

Experimentation (III)



- Wisconsin Dataset:
  - Reach the trade-off between functional and non functional quality with a 8-Anonymization

Experimentation (IV)



- Wisconsin Dataset:
  - Reach the trade-off between functional and non functional quality with a 8-Anonymization

Conclusions and future work

- Conclusions
  - □ TDA achieves a trade off between privacy and functional suitability.
  - □ TDA allows provider the releasing of useful datasets for developing AI tools
- Future Work
  - □ Evaluation in more case studies and techniques
  - □ Automation the approach
  - □ Evaluate the dependence between TDA and AI algorithms

This work was supported in part by the Spanish Ministry of Economy and Competitiveness under TestEAMoS (TIN2016-76956-C3-1-R) project and ERDF funds.

Any Question?

Cristian Augusto, Jesús Morán, Claudio de la Riva and Javier Tuya

Software Engineering Research Group

http://giis.uniovi.es

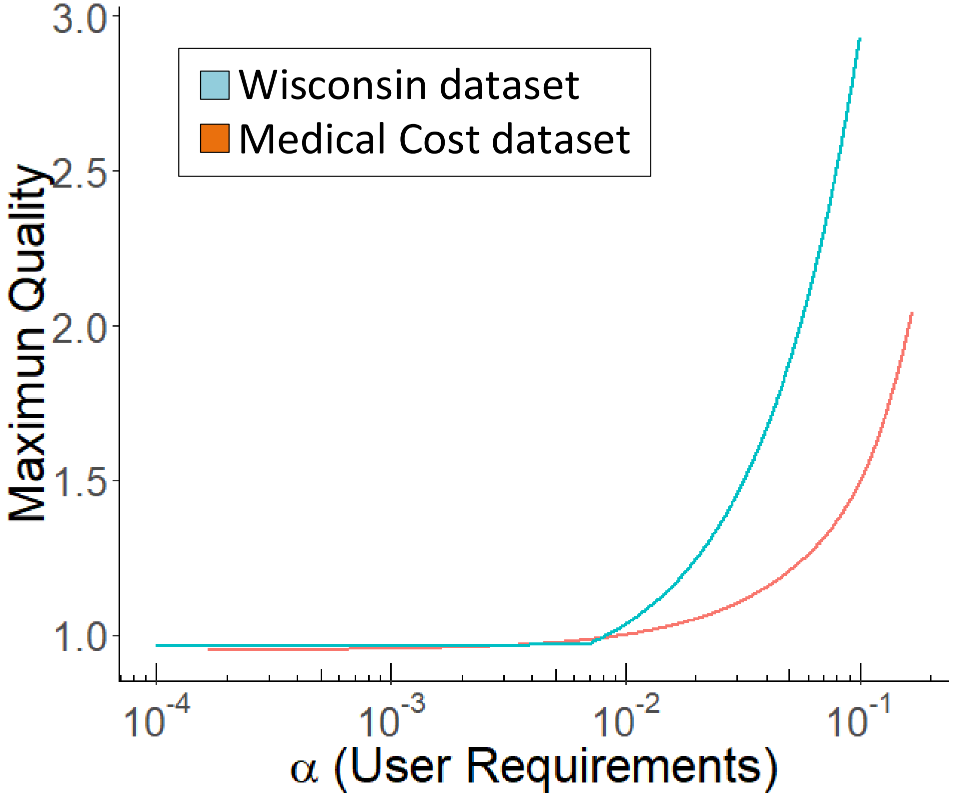
Universidad of Oviedo

User Preferences

- Represented by α value
  - Prior data utility or data privacy.
- Our quality metric :
  - $Q = QF + \alpha \cdot QNF$

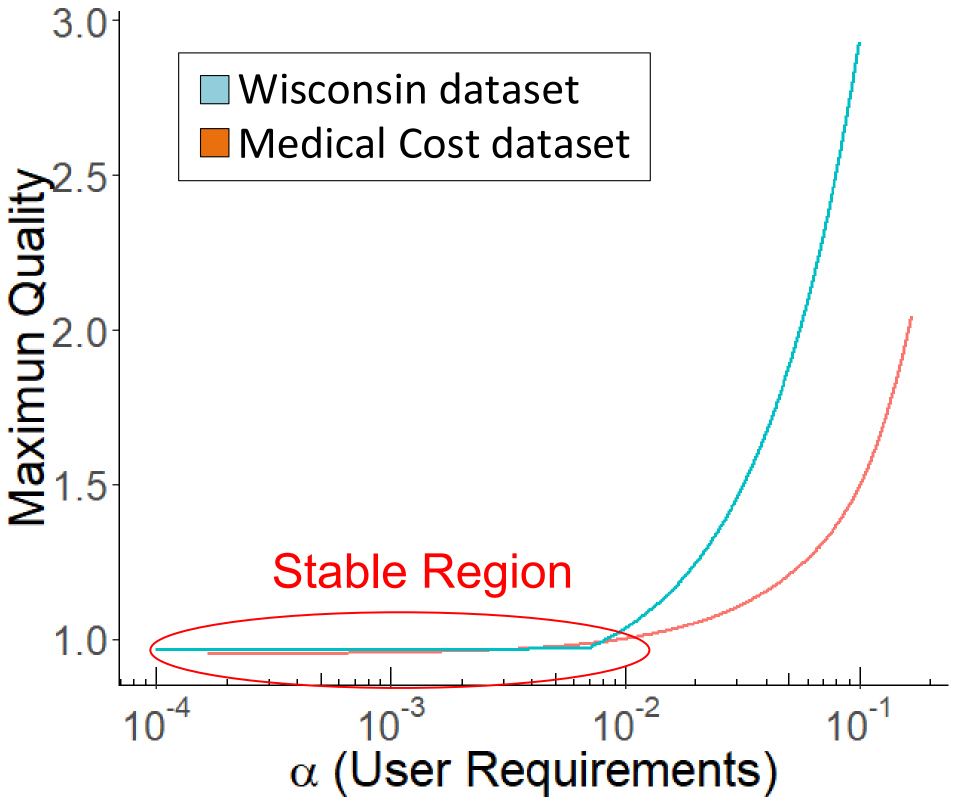
User Requirements

- Selecting the value:



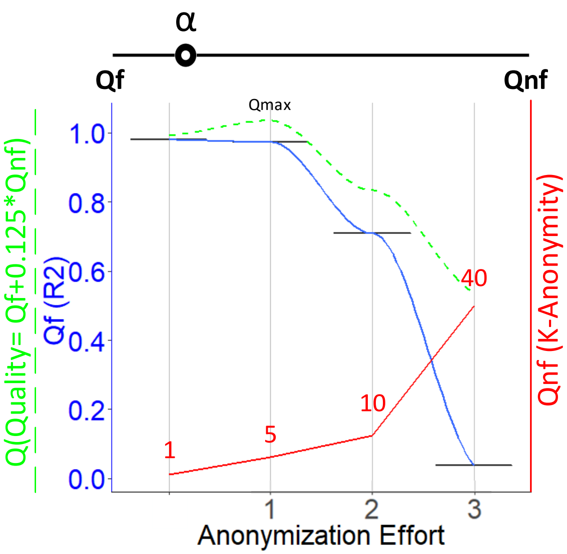
User Requirements

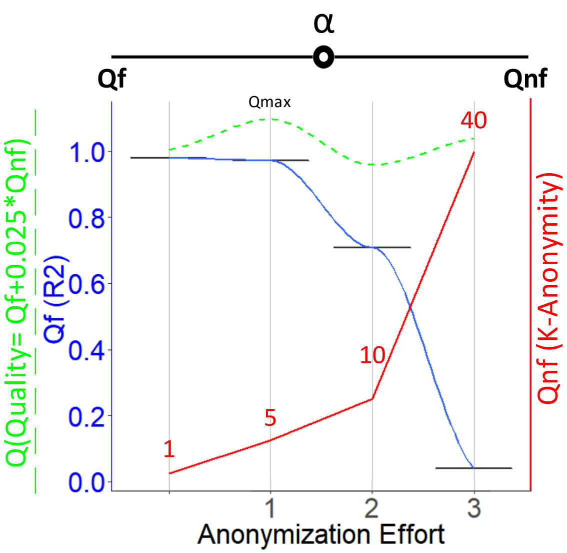
- Selecting the value:

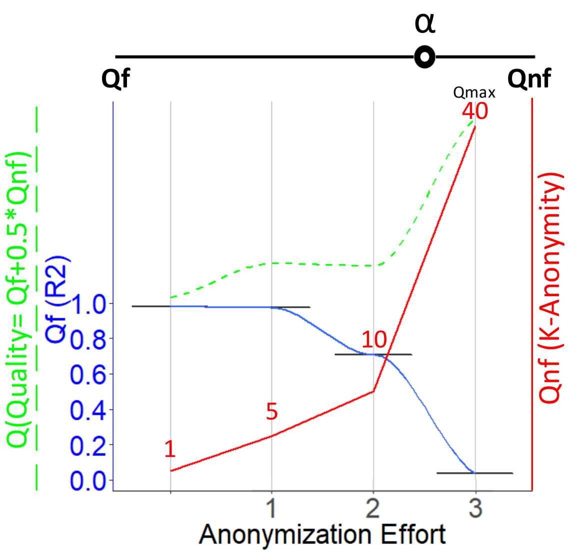


User Preferences

- Different preferences:

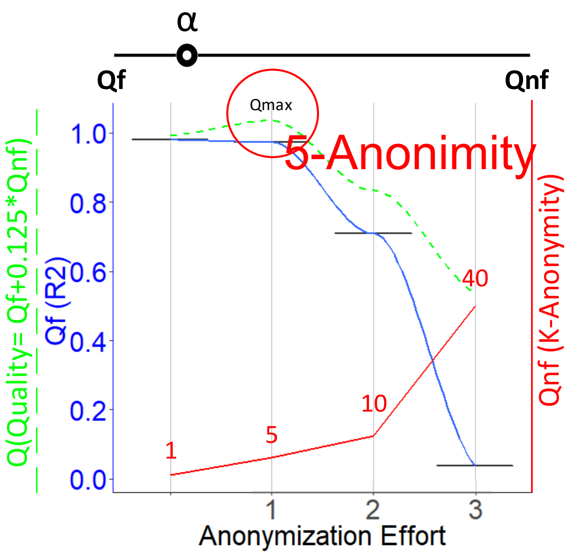


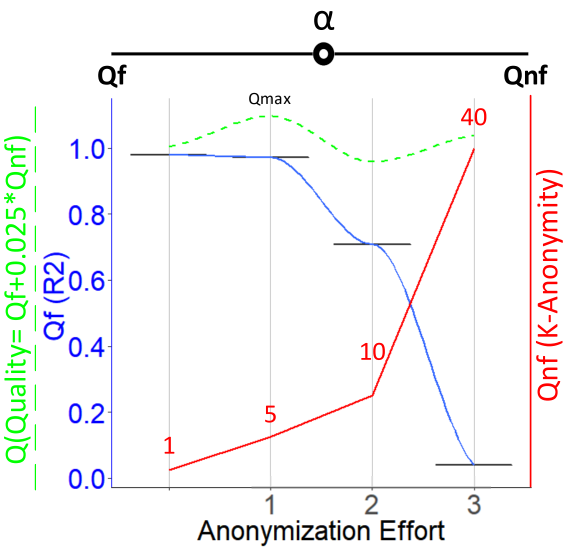


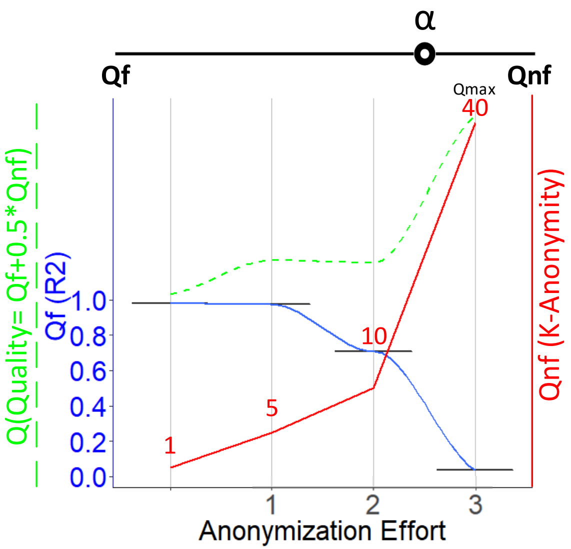


User Preferences

- Different preferences:

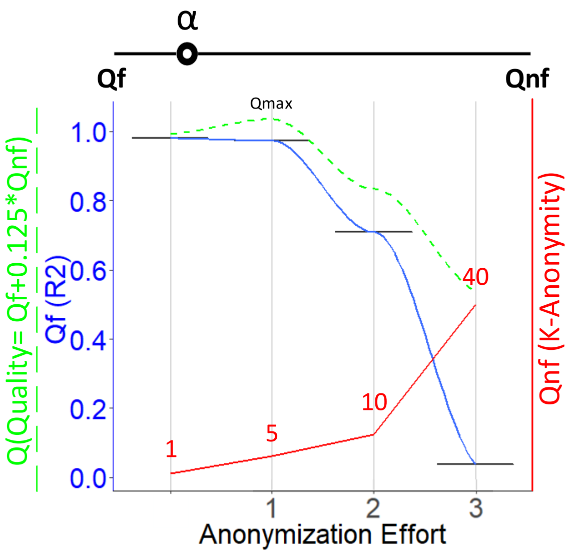


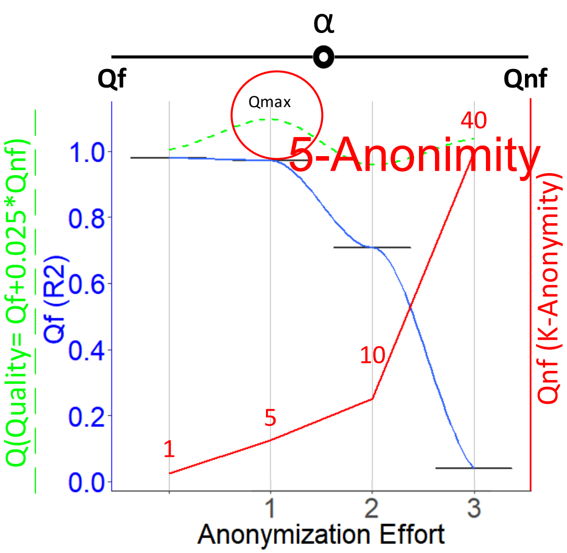


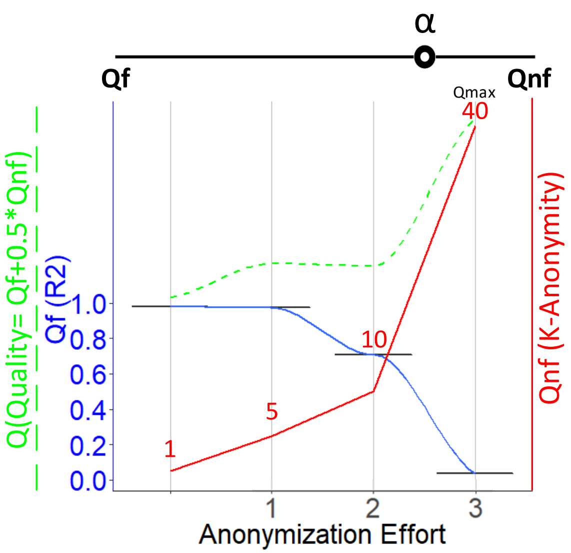


User Preferences

- Different preferences:

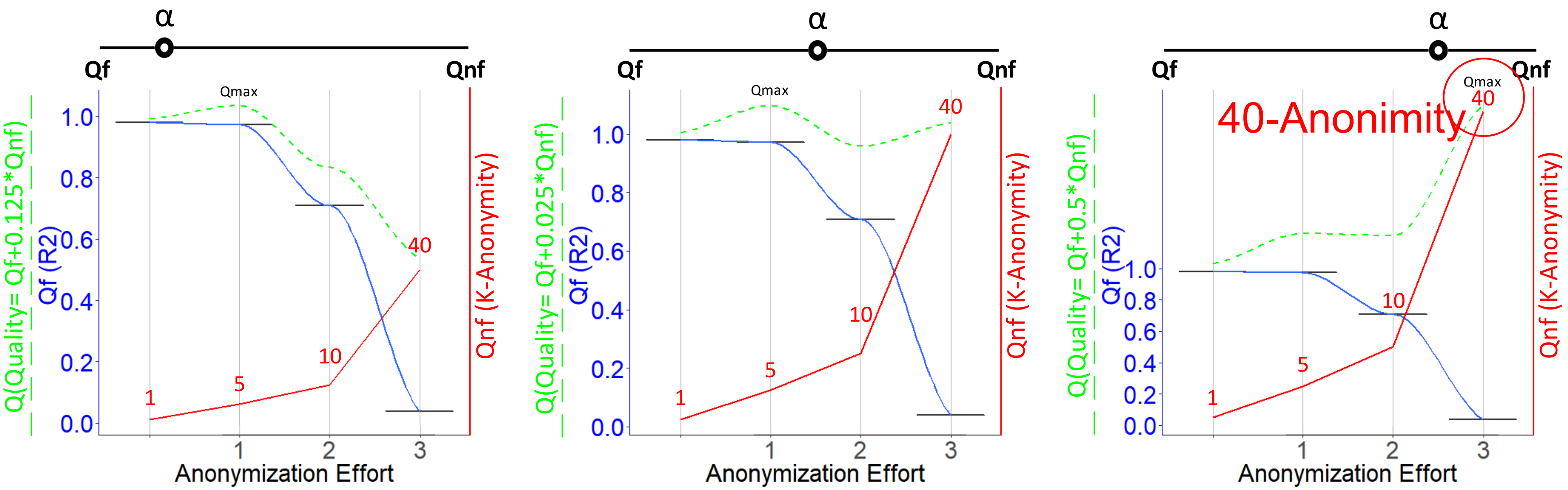






User Preferences

- Different preferences:


α
Qf
Qnf
Qmax
Q(Quality= Qf+0.125*Qnf)
Qf (R2)
Qnf (K-Anonymity)
Anonymization Effort
α
Qf
Qnf
Qmax
Q(Quality= Qf+0.025*Qnf)
Qf (R2)
Qnf (K-Anonymity)
Anonymization Effort
α
Qf
Qnf
Qmax
40-Anonimity
Q(Quality= Qf+0.5*Qnf)
Qf (R2)
Qnf (K-Anonymity)
Anonymization Effort